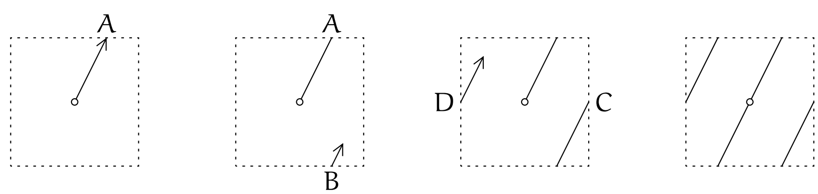
Counting intersections of spirals on a torus

1 The problem

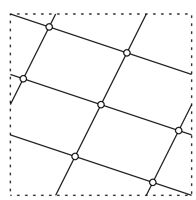
Consider a unit square with opposite sides identified. For example, if we leave the centre of the square traveling along a line of slope 2 (as shown in the first figure below), we shortly arrive at point A, which is $\frac{3}{4}$ of the way along the top side. We identify this point with — that is, consider it to be the same point as — point B, which is $\frac{3}{4}$ of the way along the bottom side. Thus (as shown in the second figure) upon passing through the top side at A we emerge from the bottom side at B.



Similarly, on passing through point C, we emerge at point D (third figure), because the left and right sides are identified. Continuing in this manner, we eventually return to the centre of the square (last figure).

The collection of points formed by such travel is not what we usually call a "line"; we will call it a "spiral". (This one, at least, "wraps around" the square a few times.)

Add to the last figure above a second spiral, also passing through the centre of the square, but of slope $-\frac{1}{3}$.



Note that, since opposite sides of the square are identified, the four corners are all the same point. Thus, when passing through a corner on constant bearing, we emerge from the opposite corner.

As the latest figure shows, these two spirals have 7 intersection points. We will show that the number of intersection points in such figures is (with a few qualifications) given by the determinant formed by the spirals' slopes:

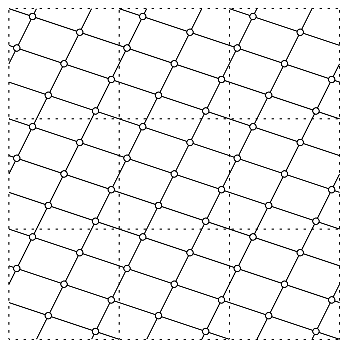
$$\begin{vmatrix} 2 & -1 \\ 1 & 3 \end{vmatrix} = 7\,.$$

The proof uses only some elementary analytic geometry and linear algebra, and one theorem of number theory (stated as proposition 6, on page 4).

2 Formulation on the plane

The square with opposite sides identified is a less familiar environment than the Cartesian plane; we would prefer to reformulate the problem on the plane so we can deploy our knowledge of that surface.

We will do so by tiling the plane with copies of the square.



This tiling induces an equivalence relation on the plane: points occupying the same position in different squares are in a certain sense the "same". For example, when counting intersections we will want to treat all the centres of these squares as just one intersection.

Recalling that the square is a unit square, we see that in this sense, any point is the "same" as the point one unit to the right, and the point one unit up, and the point two units up and three left, and in general, any integer amount left/right and any integer amount up/down. Thus we have the following definition.

Definition 1 Let $\sim$ be the binary relation on $\mathbb{R}^2$ given by

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \sim \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \iff x_1 - x_2 \in \mathbb{Z} \text{ and } y_1 - y_2 \in \mathbb{Z}\,.$$

When $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \sim \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$, we say that $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ and $\begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ are *equivalent*.

It is easy to verify that $\sim$ thus defined is indeed an equivalence relation.

It might now be natural to define a "spiral" in the plane as consisting of such-and-such points in one of the squares, and all points equivalent to those. But there is a more convenient definition, based on the observation that the line segments in each square in the tiling join up with the line segments in the neighbouring squares, as seen in the figure above. In the example on the previous page, the jump from point A to point B is a jump down by one unit; but in the tiling, jumping down one unit from point A moves us to point A of the next square down. Thus the line segment in one square that starts at B will join up with the line segment ending at A in the next square down, forming a larger line segment.

The same thing happens at all the points where a spiral crosses from one square to another, so a spiral's line segments join up on the whole plane to form a set of parallel lines. Accordingly we will define a spiral in the plane as consisting, not of certain points in one of the squares (and all equivalent points), but of a line in the plane (and all equivalent points).

For the purposes of this note, namely counting intersection points, we can restrict our attention to certain kinds of line. First, we will consider only lines that pass through the origin: if two spirals under consideration intersect at all, we can take one of their intersection points as the origin; if they don't intersect we are not very interested in them.

Second, we will consider only lines with rational slope. Since a line through the origin passes through the point (m, n) if and only if its slope is n/m, having rational slope is the same as passing through some lattice point other than the origin. (A lattice point is a point with integer coordinates.) On the tiled plane, the lattice points are all equivalent to each other, so in terms of the square with opposite sides identified, having rational slope is the same as returning to one's starting point. So the restriction to lines with rational slope assures us that the spiral will not pass through the square infinitely many times (which would make infinitely many intersection points).

Actually, "rational slope" is slightly imprecise; our definitions should allow a vertical line through the origin (that is, the y-axis), which certainly returns to its starting point, even though its slope is $1/0$, which is not a rational number.

Definition 2 (a, b) is a *coprime pair* if and only if a and b are integers and $\gcd(a, b) = 1$.

Recall that $\gcd(a, 0) = a$ for any a, so in particular, $\gcd(0, 0) = 0$; thus $(0, 0)$ is not a coprime pair. But $(1, 0)$ and $(0, 1)$ are.

Definition 3 If (a, b) is a coprime pair, then $L(a, b)$ is the line given by

$$\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in L(a, b) \iff ax + by = 0 .$$

$L(a, b)$ is the line through the origin with slope $-a/b$ (except that b may be zero, in which case the line is vertical), and $-a/b$ is not only rational but in lowest terms.

Now we can define spirals as planned: a spiral consists of points that are equivalent to the points on a certain line.

Definition 4 If (a, b) is a coprime pair, then the *spiral* $S(a, b)$ is the subset of the plane given by

$$\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in S(a, b) \iff \left\langle \exists u, v \colon \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \text{ and } \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \in L(a, b) \right\rangle .$$

(The angled brackets around the existential statement show explicitly the scope of the dummy variables u and v.)

The intersections of two spirals on the plane are, then, the elements of the set $S(a, b) \cap S(c, d)$. However, we don't wish to count that set, since it contains infinitely many "copies" of each intersection point (considering equivalent points on the plane as "copies" of the same point on the square with opposite sides identified). Leaving aside for now the question of how we will count each intersection point only once, we can at least state the question:

Given coprime pairs (a, b) and (c, d), how many nonequivalent points are there in $S(a, b) \cap S(c, d)$?

3 Preliminaries

We will need two familiar results, which we state formally here for clarity. Their proofs are omitted, since they are well-known and can be found in introductions to the relevant subjects.

From analytic geometry we know that the line $L(a, b)$, being the locus of the equation $ax+by = 0$, has the direction vector $\left[\begin{smallmatrix} -b \\ a \end{smallmatrix}\right]$; in other words, $L(a, b)$ consists of the multiples of $\left[\begin{smallmatrix} -b \\ a \end{smallmatrix}\right]$.

Proposition 5 If (a, b) is a coprime pair, then

$$\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in L(a, b) \iff \left\langle \exists s\colon \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = s\left[\begin{smallmatrix} -b \\ a \end{smallmatrix}\right] \right\rangle .$$

From number theory we know that, for any two integers, their integer linear combinations are precisely the multiples of their greatest common divisor.

Proposition 6 For any integers a and b, and any real number x,

$$\left\langle \exists m, n\colon m \in \mathbb{Z} \text{ and } n \in \mathbb{Z} \text{ and } x = am + bn \right\rangle \iff \gcd(a, b) \text{ divides } x .$$

(This proposition would usually be stated only for integers x; the generalization to real x is trivial.)

We will also need the following corollary of proposition 6.

Proposition 7 If (a, b) is a coprime pair, then for any real number x,

$$ax \in \mathbb{Z} \text{ and } bx \in \mathbb{Z} \implies x \in \mathbb{Z} .$$

Proof Suppose (a, b) is a coprime pair, so that $\gcd(a, b) = 1$. Then certainly $\gcd(a, b)$ divides 1, so by proposition 6, there exist integers m and n such that $am + bn = 1$. Thus

$$x = x1 = x(am + bn) = (ax)m + (bx)n ,$$

which is an integer if ax and bx are. □

4 Solution

Definition 4 characterizes the points in a spiral in a natural way, as the points equivalent to a certain line. Exploiting proposition 6 yields a simpler, if perhaps less intuitive, characterization of these points.

Proposition 8 If (a, b) is a coprime pair, then

$$\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in S(a, b) \iff ax + by \in \mathbb{Z}\,.$$

Proof If (a, b) is a coprime pair, then

$$\begin{aligned}
& \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in S(a, b) \\
\iff & \qquad \{\text{definition } 4\} \\
& \left\langle \exists u, v \colon \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \text{ and } \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \in L(a, b) \right\rangle \\
\iff & \qquad \{\text{definition } 1\} \\
& \left\langle \exists u, v \colon x - u \in \mathbb{Z} \text{ and } y - v \in \mathbb{Z} \text{ and } \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \in L(a, b) \right\rangle \\
\iff & \qquad \{\text{reindex the quantification; let } m, n := x - u, y - v\} \\
& \left\langle \exists m, n \colon m \in \mathbb{Z} \text{ and } n \in \mathbb{Z} \text{ and } \left[\begin{smallmatrix} x-m \\ y-n \end{smallmatrix}\right] \in L(a, b) \right\rangle \\
\iff & \qquad \{\text{definition } 3\} \\
& \left\langle \exists m, n \colon m \in \mathbb{Z} \text{ and } n \in \mathbb{Z} \text{ and } a(x - m) + b(y - n) = 0 \right\rangle \\
\iff & \qquad \{\text{algebra}\} \\
& \left\langle \exists m, n \colon m \in \mathbb{Z} \text{ and } n \in \mathbb{Z} \text{ and } ax + by = am + bn \right\rangle \\
\iff & \qquad \{\text{proposition } 6\text{, with } x := ax + by\} \\
& \gcd(a, b) \text{ divides } ax + by \\
\iff & \qquad \{\text{by hypothesis, } (a, b) \text{ is a coprime pair; definition } 2\} \\
& 1 \text{ divides } ax + by \\
\iff & \qquad \{\text{all and only the integers are divisible by } 1\} \\
& ax + by \in \mathbb{Z}
\end{aligned}$$

□

As formulated above, the problem is to count the nonequivalent points in $S(a, b) \cap S(c, d)$. A typical way to count nonequivalent objects is to restrict our attention to a complete (or complete enough) system of equivalence class representatives — in other words, a set of points such that every point we are interested in is equivalent to exactly one of the points in the set. (Having at least one equivalent point in the set ensures we count everything of interest; having at most one ensures we don't count anything twice.) The obvious choice is the unit square

$$[0, 1)^2 = \{\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] : 0 \le x < 1 \text{ and } 0 \le y < 1\}\,,$$

but we will use another, described by the next proposition.

Proposition 9 If (a, b) is a coprime pair, then every point in $S(a, b)$ is equivalent to exactly one point of the form $t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right]$ with $0 \le t < 1$, and every point of that form is in $S(a, b)$.

Proof First we show that such t exists for any point in $S(a, b)$. Note that

$$\begin{aligned}
& \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in S(a,b) \\
\iff & \qquad \{\text{definition 4}\} \\
& \left\langle \exists u, v\colon \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}u\\v\end{smallmatrix}\right] \text{ and } \left[\begin{smallmatrix}u\\v\end{smallmatrix}\right] \in L(a,b) \right\rangle \\
\iff & \qquad \{\text{proposition 5}\} \\
& \left\langle \exists u, v\colon \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}u\\v\end{smallmatrix}\right] \text{ and } \left\langle \exists s\colon \left[\begin{smallmatrix}u\\v\end{smallmatrix}\right] = s\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \right\rangle \right\rangle \\
\iff & \qquad \{\text{logic}\} \\
& \left\langle \exists s\colon \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \sim s\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \right\rangle \\
\iff & \qquad \{\text{definition 1}\} \\
& \left\langle \exists s\colon x + bs \in \mathbb{Z} \text{ and } y - as \in \mathbb{Z} \right\rangle
\end{aligned}$$

Choose such an s, and let $t = s - \lfloor s \rfloor$. Certainly, then, $0 \le t < 1$. Moreover,

$$x + bt = (x + bs) - b\lfloor s \rfloor \in \mathbb{Z} \quad \text{and} \quad y - at = (y - as) + a\lfloor s \rfloor \in \mathbb{Z}\,,$$

whence $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \sim t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right]$.

Next we show that such t is unique. Suppose $0 \le t_1 < 1$ and $0 \le t_2 < 1$. Then

$$\begin{aligned}
& t_1\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \text{ and } t_2\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \\
\implies & \qquad \{\sim \text{ is an equivalence relation}\} \\
& t_1\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \sim t_2\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \\
\iff & \qquad \{\text{definition 1}\} \\
& -bt_1 + bt_2 \in \mathbb{Z} \text{ and } at_1 - at_2 \in \mathbb{Z} \\
\iff & \qquad \{x \in \mathbb{Z} \iff -x \in \mathbb{Z}\} \\
& bt_1 - bt_2 \in \mathbb{Z} \text{ and } at_1 - at_2 \in \mathbb{Z} \\
\iff & \qquad \{\text{algebra}\} \\
& b(t_1 - t_2) \in \mathbb{Z} \text{ and } a(t_1 - t_2) \in \mathbb{Z} \\
\implies & \qquad \{\text{proposition 7, with } x := t_1 - t_2\} \\
& t_1 - t_2 \in \mathbb{Z} \\
\iff & \qquad \{-1 < t_1 - t_2 < 1\} \\
& t_1 - t_2 = 0 \\
\iff & \qquad \{\text{algebra}\} \\
& t_1 = t_2
\end{aligned}$$

Finally, we show that all such points are in $S(a,b)$. Indeed, $t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \in L(a,b)$ by proposition 5; since $\sim$ is reflexive, $t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \sim t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right]$. Thus $t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \in S(a,b)$ by definition 4. □

Now we are in a position to describe the intersections of two spirals.

Proposition 10 Suppose (a,b) and (c,d) are coprime pairs. Let $\Delta = \left|\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right| = ad - bc$. Then:

- If $\Delta = 0$, then $S(a,b)$ and $S(c,d)$ coincide.
- If $\Delta \neq 0$, then every point in $S(a,b) \cap S(c,d)$ is equivalent to exactly one point of the form $\frac{n}{\Delta}\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right]$, where $n \in \mathbb{Z}$ and $0 \leq \frac{n}{\Delta} < 1$.

Proof In the first case, when $\Delta = 0$, we know from linear algebra that the rows of the matrix $\left[\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right]$ are linearly dependent. Since neither row is zero (as noted after definition 2), each row is a multiple of the other. Thus, as we know from analytic geometry, $L(a,b)$ and $L(c,d)$ coincide, whence $S(a,b)$ and $S(c,d)$ also coincide.

So now suppose $\Delta \neq 0$, and consider the points in $S(a,b) \cap S(c,d)$. In fact, rather than considering all of $S(a,b)$, consider just the representative line segment described in proposition 9; that is, consider the points of the form $t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right]$, where $0 \leq t < 1$, which are also in $S(c,d)$.

$$
\begin{aligned}
& t\left[\begin{smallmatrix}-b\\a\end{smallmatrix}\right] \in S(c,d)\\
\iff & \quad \{\text{definition of scalar multiplication}\}\\
& \left[\begin{smallmatrix}-tb\\ta\end{smallmatrix}\right] \in S(c,d)\\
\iff & \quad \{\text{proposition 8}\}\\
& -tbc + tad \in \mathbb{Z}\\
\iff & \quad \{\text{definition of } \Delta\}\\
& t\Delta \in \mathbb{Z}\\
\iff & \quad \{\text{logic}\}\\
& \langle \exists n \colon n \in \mathbb{Z} \text{ and } t\Delta = n \rangle\\
\iff & \quad \{\Delta \neq 0\}\\
& \langle \exists n \colon n \in \mathbb{Z} \text{ and } t = \tfrac{n}{\Delta} \rangle
\end{aligned}
$$

So the intersection points $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$ of $S(a,b)$ and $S(c,d)$ that lie on the representative line segment described by proposition 9 are those for which

$$\begin{aligned}
&\left\langle \exists t\colon \begin{bmatrix} x \\ y \end{bmatrix} = t\begin{bmatrix} -b \\ a \end{bmatrix} \text{ and } 0 \le t < 1 \text{ and } t\begin{bmatrix} -b \\ a \end{bmatrix} \in S(c,d) \right\rangle \\
\iff &\qquad \{\text{by the calculation above}\} \\
&\left\langle \exists t\colon \begin{bmatrix} x \\ y \end{bmatrix} = t\begin{bmatrix} -b \\ a \end{bmatrix} \text{ and } 0 \le t < 1 \text{ and } \left\langle \exists n\colon n \in \mathbb{Z} \text{ and } t = \tfrac{n}{\Delta} \right\rangle \right\rangle \\
\iff &\qquad \{\text{logic}\} \\
&\left\langle \exists n\colon \begin{bmatrix} x \\ y \end{bmatrix} = \tfrac{n}{\Delta}\begin{bmatrix} -b \\ a \end{bmatrix} \text{ and } 0 \le \tfrac{n}{\Delta} < 1 \text{ and } n \in \mathbb{Z} \right\rangle
\end{aligned}$$

that is, the points described in the proposition. □

A corollary to this proposition is that if $\Delta \neq 0$ then there are $|\Delta|$ intersection points, which was what we set out to prove.

Or nearly so. In proposition 10 the relevant determinant is formed by placing the spirals' normal vectors in rows, while the initial statement of the result on page 1 placed the slopes in columns (without specifying how to handle signs). It is easy to show that these determinants differ at most in sign. The initial statement also made no mention of the need to take the absolute value of the determinant, nor of the need to express the slopes in lowest terms, nor of the meaning of a zero determinant.

5 Alternative approaches

The determinant appears in the proof of proposition 10 in a somewhat enigmatic way. Two alternative approaches, in which the determinant appears more naturally, begin with the observation that

$$\begin{aligned}
&\begin{bmatrix} x \\ y \end{bmatrix} \in S(a,b) \cap S(c,d) \\
\iff &\qquad \{\text{proposition } 8\} \\
&ax + by \in \mathbb{Z} \text{ and } cx + dy \in \mathbb{Z} \\
\iff &\qquad \{\text{matrix algebra}\} \\
&\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}^2
\end{aligned}$$

That is, the intersection points of $S(a,b)$ and $S(c,d)$ are precisely the preimages of lattice points under the linear transformation whose matrix is $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

In the first alternative approach, we consider which lattice points have preimages on the representative line segment described in proposition 9; if $\Delta \neq 0$, these are the points $\begin{bmatrix} x \\ y \end{bmatrix}$ such that

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} m \\ n \end{bmatrix} \text{ and } \begin{bmatrix} x \\ y \end{bmatrix} = t\begin{bmatrix} -b \\ a \end{bmatrix}$$

for suitable m, n, t. Equating these two expressions for $\begin{bmatrix} x \\ y \end{bmatrix}$ and applying some matrix algebra yields

$$\frac{m}{\Delta}\begin{bmatrix} d \\ -c \end{bmatrix} + \frac{n}{\Delta}\begin{bmatrix} -b \\ a \end{bmatrix} = 0\begin{bmatrix} d \\ -c \end{bmatrix} + t\begin{bmatrix} -b \\ a \end{bmatrix} .$$

Since $\Delta \neq 0$, the vectors $\left[\begin{smallmatrix} d \\ -c \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -b \\ a \end{smallmatrix}\right]$ form a basis for $\mathbb{R}^2$; identifying the corresponding coefficients yields proposition 10.

In the second alternative approach, we consider which lattice points have preimages in the unit square $[0, 1)^2$. The image of that square is a parallelogram with area $|\Delta|$ and whose vertices lie on lattice points. By Pick's theorem,

$$|\Delta| = I + \tfrac{1}{2}B - 1$$

where B is the number of lattice points on the edges of the parallelogram and I is the number of lattice points in its interior. From coprimeness it can be shown that the only points on the edges are the vertices; thus $B = 4$. The intersection points we wish to count correspond to the lattice points in the interior, plus one for the origin, that is, $I + 1$.